Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte

Schwarzenegger, Christian ; Thouvenin, Florent ; Stiller, Burkhard ; George, Damian

Other titles: Use of cloud services by lawyers

Originally published at:
Schwarzenegger, Christian; Thouvenin, Florent; Stiller, Burkhard; George, Damian (2019). Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte. Anwaltsrevue, 22(1):25-40.

Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte

Schwarzenegger, Christian ; Thouvenin, Florent ; Stiller, Burkhard ; George, Damian

NUTZUNG VON CLOUD-DIENSTEN DURCH ANWÄLTINNEN UND ANWÄLTE

CHRISTIAN SCHWARZENEGGER
Prof. Dr., RA, Universität Zürich

FLORENT THOUVENIN
Prof. Dr., RA, Universität Zürich

BURKHARD STILLER
Prof. Dr., Universität Zürich

DAMIAN GEORGE
RA, MLaw, Universität Zürich

Stichworte: Cloud-Computing, Berufsgeheimnis, Datenschutzrecht

Die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte wirft straf- und datenschutzrechtliche Fragen auf, die in der Lehre teilweise kontrovers beurteilt werden. Der Beitrag zeigt auf, dass solche Dienste von Anwältinnen und Anwälten grundsätzlich ohne Weiteres genutzt werden dürfen. Der Beitrag ist die Kurzfassung eines Gutachtens, das die Autoren im Herbst 2018 für den Schweizerischen Anwaltsverband erstellt haben. Das Gutachten wird im Volltext in der Reihe des Center for Information Technology, Society, and Law (ITSL) der Universität Zürich publiziert.

I. Einleitung

Die Nutzung von IT-Diensten ist aus der Anwaltspraxis längst nicht mehr wegzudenken. Das Aufsetzen und die Wartung der IT werden allerdings oft nicht durch die Anwältin oder den Anwalt selbst vorgenommen, sondern internen IT-Mitarbeitenden oder einem externen IT-Dienstleister übertragen. In jüngerer Zeit nutzen Anwaltskanzleien nicht nur sogenannte Stand-alone-Computer oder lokale Netzwerke, sondern auch die Dienste von Cloud-Providern. Der Begriff «Cloud» beschreibt dabei eine Reihe von Onlinediensten, die über ein Netzwerk von beliebigen Orten aus zugänglich sind, sodass ihr physischer Standort in technischer Sicht vernachlässigt werden kann.

Diese Entwicklung wirft die Frage auf, ob und gegebenenfalls unter welchen Voraussetzungen in der Schweiz tätige Anwältinnen und Anwälte im Rahmen der Ausübung ihrer beruflichen Tätigkeit für das Bearbeiten, Speichern und Archivieren von Dokumenten und anderen Dateien Cloud-Dienste nutzen dürfen. Zur Beantwortung dieser Frage ist zu prüfen, ob die Nutzung von Cloud-Diensten eine Verletzung des Berufsgeheimnisses nach Art. 321 StGB darstellt (III) und mit den Vorgaben des Datenschutzrechts vereinbar ist (IV). Vorab sind jedoch die technischen Grundlagen zu klären (II).

II. Technische Grundlagen

1. Cloud-Dienst-Modelle

Nahezu alle IT-Ressourcen können in eine Cloud ausgelagert werden und entsprechend unterschiedlich sind die am Markt angebotenen Cloud-Dienst-Modelle. Meist werden drei Hauptkategorien unterschieden: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS). Das PaaS-Dienst-Modell wird dabei vor allem zur Entwicklung von Applikationen eingesetzt. Da Anwaltskanzleien dieses Modell gegenwärtig kaum nutzen werden, beschränkt sich die nachfolgende Darstellung auf die beiden anderen Modelle.

A) Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a-Service (IaaS) ist das Grundmodell der Dienstleistungen einer Cloud. Beim IaaS-Dienst-Modell werden die Cloud-Computing-Ressourcen (z. B. Rechnen, Speichern oder Netzwerkzugang) als Dienstleistung zur Verfügung gestellt. Dieses Modell ist eine interessante Option, wenn eine Anwaltskanzlei eine rechnergestützte Infrastruktur benötigt, diese aber aus Kostengründen nicht selbst betreiben möchte. Die Anwaltskanzlei bestimmt in diesem Modell weiterhin, welche Softwarelösungen auf der Infrastruktur installiert werden, und muss

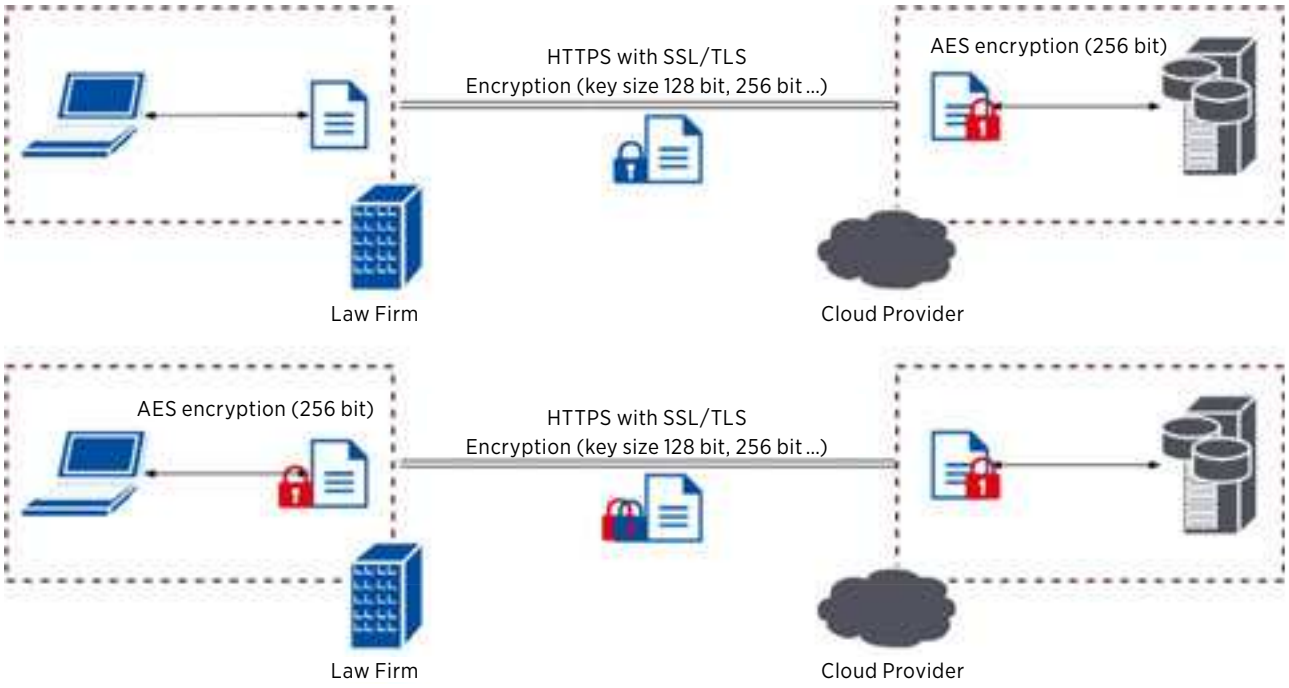

Abbildung 1: Verschlüsselung und Schlüsselverwaltung im IaaS-Dienst-Modell

auch Massnahmen treffen, welche die Vertraulichkeit und Integrität des Systems gewährleisten. Der Cloud-Provider dagegen hat dafür zu sorgen, dass die von der Anwaltskanzlei gespeicherten Daten jederzeit verfügbar sind.

B) Software-as-a-Service (SaaS)

Bei Software-as-a-Service (SaaS) stellt der Cloud-Provider eine endverbraucherfreundliche, webbasierte Softwareanwendung zur Verfügung. Bei diesem Dienst-Modell werden nicht nur Software und Daten auf der Cloud-Infrastruktur zentral gespeichert, sondern es findet auch die Datenverarbeitung auf dieser Infrastruktur statt (z. B. Textverarbeitung, Kalkulation oder Erstellen von Präsentationen). Der Cloud-Provider installiert ausserdem Updates und bietet Supportfunktionen an. Im Gegensatz zu IaaS kann die Anwaltskanzlei beim SaaS-Dienst-Modell nur beschränkt sicherheitsrelevante Konfigurationen vornehmen. In technischer Hinsicht hat sie nur für die Sicherheit der Zugangsdaten zu sorgen. Die Vertraulichkeit der Daten, die Integrität des Netzwerks und die Verfügbarkeit der Dienste hat der Cloud-Provider sicherzustellen.

2. Datenzugriff

Bei der Nutzung von Cloud-Diensten werden die Daten nicht mehr lokal in der Anwaltskanzlei, sondern beim Cloud-Provider gespeichert. Die Übertragung über das Internet erfolgt dabei verschlüsselt und zwar unter Verwendung von HTTPS (Hypertext Transmission Protocol Secure) und TLS (Transport Layer Security)[1], das eine starke Schlüsselgrösse (128 oder 256 bit) einsetzt. Beim Cloud-Provider werden die Daten zudem mit einem lokalen Schlüssel verschlüsselt, z. B. mit dem AES-(Advanced-Encryption-Standard-)Verschlüsselungsverfahren.

Beim Iaas-Dienst-Modell sind zwei Varianten zu unterscheiden: Werden die Daten erst beim Cloud-Provider verschlüsselt, haben die Anwaltskanzlei und der Cloud-Provider Zugang zu den Daten im Klartext (siehe oberen Teil von Abbildung 1). Die beim Cloud-Provider zu speichernden Daten können aber schon vor der Übertragung über das Internet durch die Anwaltskanzlei verschlüsselt werden (siehe unteren Teil von Abbildung 1). Damit hat nur noch die Anwaltskanzlei Zugang zu den Daten.

Im SaaS-Dienst-Modell (Abbildung 2) stellt der Cloud-Provider die Software in der Cloud zur Verfügung. Die Softwareapplikation muss dabei auf die unverschlüsselten Dateien zugreifen können und die Daten sind deshalb für den Cloud-Provider im Klartext sichtbar. Andere Nutzer derselben Cloud können allerdings nicht auf die Daten zugreifen, weil für jeden Kunden ein anderer Schlüssel verwendet wird. Kunden, die mit vertraulichen Inhalten arbeiten, müssen sich bei der Nutzung von SaaS aber bewusst sein, dass der Cloud-Provider auf ihre Daten zugreifen kann und an sich die Möglichkeit hat, diese auch zu nutzen.

III. Strafrechtliche Beurteilung: Verletzung des Berufsgeheimnisses

Gemäss Art. 321 StGB werden Berufsgeheimnisträger und deren Hilfspersonen (III. 2) auf Antrag bestraft, wenn sie ein geschütztes Geheimnis (III. 1) einem unberechtigten

1 TLS ist die aktualisierte Version von SSL (Secure Socket Layer) 3.0. SSL 3.0 wurde von der IETF (Internet Engineering Task Force) im Dokument RFC 7568 als veraltet eingestuft.

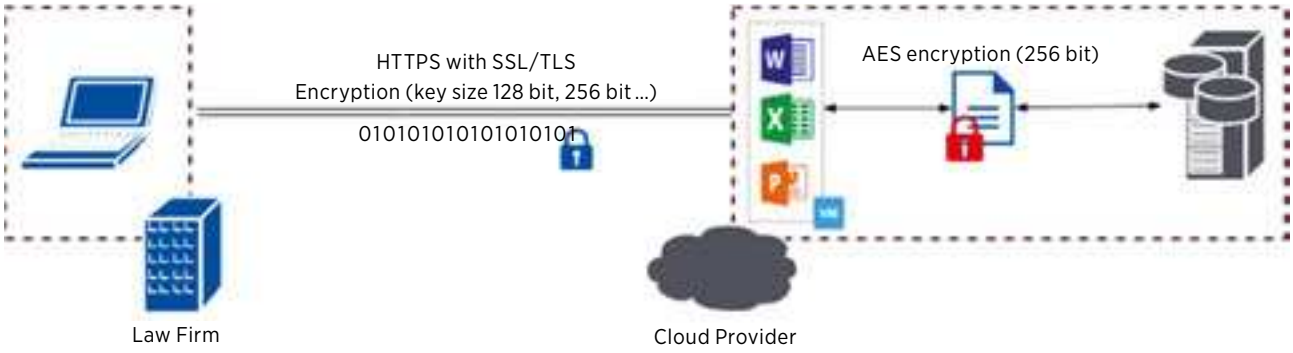

Abbildung 2: Verschlüsselung und Schlüsselverwaltung im SaaS-Dienst-Modell

Dritten offenbaren (III. 3) und dabei vorsätzlich und ohne Rechtfertigungsgrund handeln.

1. Angriffsobjekt: das geschützte Geheimnis

Rechtlichen Schutz geniessen materielle Geheimnisse. Ein Geheimnis ist jede relativ unbekannte Tatsache. Relative Unbekanntheit ist gegeben, wenn nur eine beschränkte Anzahl von Personen über die fraglichen Informationen verfügt. Ein materielles Geheimnis liegt vor, wenn der Geheimnisherr ein berechtigtes Interesse an der Geheimhaltung hat, das er gewahrt haben will.[2] Art. 321 StGB erfasst alle Informationen, die der Anwältin oder dem Anwalt infolge ihres bzw. seines Berufes anvertraut wurden, sowie alle Informationen, die sie oder er bei der Ausübung des Berufes wahrgenommen hat. Die Informationen müssen sich weder auf den Klienten beziehen noch müssen sie der Anwältin oder dem Anwalt bewusst mitgeteilt oder übergeben worden sein.[3] Nicht unter das Berufsgeheimnis gemäss Art. 321 Ziff. 1 Abs. 1 StGB fallen Informationen aus der sogenannten akzessorischen anwaltlichen Geschäftstätigkeit, also aus der Vermögensverwaltung, aus Depotgeschäften, Inkassomandaten und Verwaltungsratsmandaten[4] oder aus dem Privatleben der Anwältin oder des Anwalts.

2. Täter: Geheimnisträger und Hilfspersonen

A) Geheimnisträger

Art. 321 StGB ist ein echtes Sonderdelikt; taugliche Täter sind deshalb nur die explizit und abschliessend aufgezählten Berufsangehörigen.[5] Anwälte werden in der Bestimmung ebenso namentlich erwähnt wie Verteidiger[6], Notare und Patentanwälte sowie weitere Berufsgruppen.[7] Zur Kategorie der Anwälte zählen alle Personen, die eine entsprechende fachliche Ausbildung abgeschlossen haben und über einen schweizerischen oder ausländischen Fähigkeitsausweis verfügen, wobei es keine Rolle spielt, ob sie im anwaltschaftlichen Monopolbereich tätig sind oder nicht.[8] Auch auf den Eintrag im kantonalen Anwaltsregister kommt es nicht an.[9]

B) Hilfspersonen

Hilfspersonen im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB haben die gleiche Pflicht zur Geheimhaltung wie der (Haupt-)Geheimnisträger. Für die vorliegende Fragestellung ist die Auslegung des Begriffs der Hilfsperson eines zur Geheimhaltung verpflichteten Berufsangehörigen entscheidend. Die Bedeutung dieses Begriffs muss anhand der anerkannten Auslegungsmethoden ermittelt werden.

Nach der grammatikalischen Auslegung sind Hilfspersonen Individuen, die jemanden bei der Erfüllung einer Aufgabe unterstützen. Der Wortsinn erfasst alle möglichen Hilfstätigkeiten, seien es Schreibarbeiten, Recherchen, Botengänge oder die Unterstützung bei der

2 Vgl. BGE 127 IV 122, E. 1; 142 IV 65, E. 5.1 je m. w. H. (zu Art. 320 StGB); NIGGLI, Gutachten betreffend Anwendung von Art. 321 StGB auf angestellte Unternehmensjuristen (In-house lawyers), Freiburg 2005, www.swissholdings.ch/fileadmin/kundendaten/Dokumente/Archiv_Publikationen-Publikation/05-08-05-Gutachten_Niggli.pdf, zuletzt besucht am 19. Dezember 2018, 20 ff. m. w.H; OBERHOLZER, in: Basler Kommentar Strafrecht II, 3. Aufl., Basel 2013, StGB 321 N 14; STRATENWERTH/BOMMER, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7. Aufl., Bern 2013, § 61 N 5; TRECHSEL/VEST, in: Schweizerisches Strafgesetzbuch, Praxiskommentar, 3. Aufl., Zürich 2018, StGB 321 N 20 ff. m. w. H.

3 So schon GAUTIER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, Luzern 1915, Bd. 4, 365; NIGGLI, Unterstehen dem Berufsgeheimnis nach Art. 321 StGB auch Unternehmensjuristen? Eine Verteidigung des materiellen Strafrechts gegen die Freunde des Verfassungsrechts, zugleich eine Antwort auf Pfeifer, AwR 2006, 279; OBERHOLZER (Fn. 2), StGB 321 N 16; TRECHSEL/VEST (Fn. 2), StGB 321 N 21 f.

4 Vgl. BGE 143 IV 462, E. 2.2; NIGGLI (Fn. 2), 21 ff.; TRECHSEL/VEST (Fn. 2), StGB 321 N 21. Strafrechtlichen Schutz soll nur die anwaltstypische Tätigkeit geniessen, wobei die Abgrenzungen in der Praxis schwierig sind (siehe zur Auslagerung von GwG-Compliance-Aufgaben an eine Anwaltskanzlei: BGer 1B_85/2016 vom 20. September 2016, E. 6).

5 ZÜRCHER, Schweizerisches Strafgesetzbuch, Erläuterungen zum Vorentwurf vom April 1908, Bern 1914, 351; OBERHOLZER (Fn. 2), StGB 321 N 11; TRECHSEL/VEST (Fn. 2), StGB 321 N 3; STRATENWERTH/BOMMER (Fn. 2), § 61 N 17; WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zürich 2016, 13.

6 Die Verteidigung von Personen, die eines Verbrechens oder Vergehens beschuldigt werden, ist gemäss StPO Anwälten vorbehalten, die nach dem BGFA berechtigt sind, Parteien vor Gerichtsbehörden zu vertreten (Art. 2 BGFA, Art. 127 Abs. 5 StPO). Die zusätzliche Erwähnung von Verteidigern hat somit nur noch im Übertretungsstrafverfahren eine eigenständige Bedeutung.

7 Zu den einzelnen Berufsgruppen näher OBERHOLZER (Fn. 2), StGB 321 N 5 ff.; TRECHSEL/VEST (Fn. 2), StGB 321 N 6 ff.

8 NIGGLI (Fn. 2), 15, 19 f.

9 OBERHOLZER (Fn. 2), StGB 321 N 6.

Datenverwaltung. Auch IT-Dienstleister, die für den Geheimnisträger Daten bearbeiten, können ohne Weiteres unter diesen Begriff gefasst werden.

In systematischer Hinsicht fällt auf, dass die Hilfspersonen in Art. 321 Ziff. 1 Abs. 1 StGB in einem Atemzug mit den Kategorien der (Haupt-)Geheimnisträger genannt und der gleichen Strafdrohung unterworfen werden. Dies deutet an, dass der Gesetzgeber den Kreis der Personen, die das Geheimnis zur Kenntnis nehmen, breit fassen wollte, weil er von einer funktionalen arbeitsteiligen Umgebung ausging.

Klare Hinweise ergeben sich auch aus der historischen Auslegung. Die Gesetzesmaterialien verdeutlichen, dass ein restriktives Verständnis des Begriffs der Hilfsperson explizit abgelehnt wurde. Die Zweifel zweier Mitglieder der Expertenkommission, die eine engere Begriffsfassung befürworteten, wurden zur Kenntnis genommen, aber bewusst nicht berücksichtigt.[10] Auch in der parlamentarischen Beratung führte der Hinweis, dass die Bezeichnung «Gehilfen solcher Personen» etwas vage sei, zu keiner Diskussion oder gar Anpassung der Strafbestimmung.[11]

Auch aus teleologischer Sicht macht es keinen Sinn, den Kreis der Hilfspersonen eng zu begrenzen. Denn bei einer engen Begriffsdefinition müsste der Geheimnisträger alle geheimen Dokumente selbst einschliessen bzw. verschlüsseln, die IT-Betriebssysteme selbst warten und die Datenverwaltung selbst besorgen, um die Möglichkeit des Zugriffs von unberechtigten Dritten – z. B. Reinigungspersonal, Sekretariat oder IT-Mitarbeitern – auszuschliessen. Es kann aber nicht Sinn und Zweck des Gesetzes sein, betrieblich praktisch unmögliche oder zumindest höchst ineffiziente Prozesse zu fordern.[12]

Der schweizerische Berufsgeheimnisschutz folgt somit einem breit gefassten, funktionalen Verständnis der Hilfsperson.[13] Hilfsperson im Sinn von Art. 321 StGB ist, wer bei der Berufstätigkeit eines (Haupt-)Geheimnisträgers in einer Weise mitwirkt, die es ihr oder ihm grundsätzlich ermöglicht, von Geheimnissen Kenntnis zu nehmen.

3. Tathandlung des Offenbaren

A) Kenntnisnahme

Das objektive Tatbestandsmerkmal des Offenbarens ist erfüllt, wenn der Geheimnisträger das Geheimnis einem dazu nicht ermächtigten Dritten zur Kenntnis bringt oder diesem die Kenntnisnahme ermöglicht. Nach der Rechtsprechung des Bundesgerichts und der h. L. wird die Kenntnisnahme durch einen Dritten für die Vollendung der Tat vorausgesetzt.[14] Die Tat soll aber auch durch unechte Unterlassung begangen werden können,[15] z. B. durch eine unzureichende Aufbewahrung von Akten.[16]

Bei anonymisierten oder verschlüsselten Informationen liegt kein Offenbaren vor, weil eine Kenntnisnahme verunmöglicht wird.[17] Die Archivierung verschlüsselter Daten in der Cloud (IaaS-Dienst-Modell) erfüllt daher den objektiven Tatbestand von Art. 321 StGB nicht (siehe dazu II. 1. A). Beim SaaS-Dienst-Modell hat der Cloud-Provider hingegen technisch gesehen Zugang zu den gespeicher-

10 So wies ALFRED GAUTIER in der zweiten Expertenkommission auf Abgrenzungsprobleme hin: «Car il est délicat de délimiter le cercle de ces auxiliaires. On risque d'y comprendre de simples petits comparses sur lesquels ne doit reposer aucune responsabilité spéciale, …» (GAUTIER [Fn. 3], 365). Die Expertenkommission ging auf dieses Argument nicht näher ein. Im Einklang mit GAUTIER stellte EUGÈNE DESCHENAUX einen Antrag, der eine Änderung des Begriffs «auxiliaire» in «assistant ou employé supérieur» verlangte, um untergeordnete Angestellten von einer möglichen Strafbarkeit auszunehmen (Protokoll der zweiten Expertenkommission Strafgesetzbuch, Luzern 1915, Bd. 4, 371). Der Antrag DESCHENAUX wurde von der Expertenkommission mit grosser Mehrheit abgelehnt (*ibid.,* 376).

11 Stenographisches Bulletin, Nationalrat, 26. 9. 1929, 612.

12 Für all diese Tätigkeiten eine Einwilligung des Geheimnisherrn zu verlangen, kann aus den gleichen Überlegungen keine Lösung sein. So müssten vor jeder organisatorischen Änderung, wie bei der Einstellung von Praktikanten und Sekretariatsmitarbeitern oder der Mandatierung eines Reinigungsunternehmens, die Einwilligungserklärungen aller Klienten beigebracht werden. Dies erscheint unzweckmässig, denn der Geheimnisträger wäre in einer arbeitsteiligen Welt schnell mit einer Vielzahl von Einwilligungsersuchen konfrontiert, was zu einem blossen Abnicken der vorgelegten Erklärungen führen dürfte.

13 WOHLERS vertritt hier eine – an deutschen Quellen zu § 203 a. F. D-StGB angelehnte – enge Auslegung. Er stützt sich dabei insbesondere auf eine bisher in der schweizerischen Diskussion ungebräuchliche Rechtsfigur, nämlich den «Kreis der zum Wissen Berufenen». Damit wird zum Ausdruck gebracht, dass der Geheimnisherr eine Person oder einen Kreis von Personen bestimme, mit der oder dem er das Geheimnis teilen wolle (WOHLERS [Fn. 5], 16, 18 und 26; WOHLERS, Outsourcing durch Berufsgeheimnisträger, digma 2017, 116). Dies widerspricht allerdings Schweizer Rechtsprechung und herrschender Lehre: BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.2, «Der Kreis der Hilfspersonen ist praktisch unbegrenzt»; CHAPPUIS/ALBERINI, Secrets professionnel de l'avocat et solutions Cloud, AwR 2017, 339 f.; KELLER, Das ärztliche Berufsgeheimnis gemäss Art. 321 StGB unter besonderer Berücksichtigung der Regelung im Kanton Zürich, Diss., Zürich 1993, 106 ff. m. w. H., mit der Einschränkung auf «Berufsmässigkeit»; NIGGLI (Fn. 2), 30 f.; OBERHOLZER (Fn. 2), StGB 321 N 10; TRECHSEL/VEST (Fn. 2), StGB 321 N 13; STRATENWERTH/BOMMER (Fn. 2), § 61 N 17, mit der Einschränkung auf «Berufsmässigkeit». Vgl. NATER/ZINDEL, in: Kommentar zum Anwaltsgesetz: Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) BGFA, 2. Aufl., Zürich 2011, BGFA 13 N 51 f. und N 53: «Massgeblich ist vielmehr sowohl strafrechtlich als auch berufsrechtlich, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu geschützten Informationen einschliesst.»

14 BGer 6B_1403/2017 vom 8. August 2017, E. 1.2.2; ISENRING, StGB/JStG-Kommentar, Orell Füssli Kommentar, 20. Aufl., Zürich 2018, StGB 321 N 10b; DONATSCH/THOMMEN/WOHLERS, Strafrecht IV: Delikte gegen die Allgemeinheit, Zürcher Grundrisse des Strafrechts, 5. Aufl., Zürich 2017, 580 f.; OBERHOLZER (Fn. 2), StGB 320 N 10.

15 OBERHOLZER (Fn. 2), StGB 321 N 19; STRATENWERTH/BOMMER (Fn. 2), § 61 N 7 und 19; STRAUB, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP 2010, 552 und 555; TRECHSEL/VEST (Fn. 2), StGB 321 N 23. Wenn zur Vollendung eine Kenntnisnahme durch einen unbefugten Dritten vorausgesetzt wird, kann der Tatbestand aber nicht schon durch eine unzureichende Aufbewahrung der geheimen Informationen vollendet werden. Dies wäre allenfalls als Versuch strafbar.

16 Betreffend die Anforderungen für die Archivierung der Akten können die datenschutzrechtlichen Vorgaben aus Art. 7 DSG sowie Art. 8 VDSG herangezogen werden, da es sich bei den Akten regelmässig um Datensammlungen im Sinn des DSG handelt, die oft besonders schützenswerte Daten i. S. v. Art. 3 lit. c DSG umfassen. Anwälte sind von der Meldepflicht gemäss Art. 11a DSG befreit, vgl. BLECHTA, in: Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, DSG 11a N 14d. Zur Aufbewahrung: BLECHTA *(ibid.),* DSG 7 N 7 ff.

17 BERGER, Outsourcing vs. Geheimnisschutz im Bankgeschäft, recht 2000, 191 m. w. H.; BLATTMANN, in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012, IDG 6 N 13; TRECHSEL/VEST (Fn. 2), StGB 321 N 23; WOHLERS (Fn. 5), 20; EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER, 14. Tätigkeitsbericht 2006/2007 für den Zeitraum zwischen 1. 4. 2006 und 31. 3. 2007, 51.

ten Daten (siehe dazu II. 2). In diesen Konstellationen ist eine Kenntnisnahme deshalb möglich.

B) Kein Offenbaren gegenüber Hilfspersonen

Da der Gesetzgeber von einer arbeitsteiligen Berufsumgebung des Geheimnisträgers ausging und weil es bei funktionaler Betrachtung der Zusammenarbeit zwischen Geheimnisträger und Hilfspersonen gerade ein Definitionsmerkmal ist, dass Letztere mit den Geheimnissen in Kontakt kommen, können Hilfspersonen nie unberechtigte Dritte sein. Hilfspersonen gehören vielmehr zur arbeitsteiligen Organisation des Geheimnisträgers. Sie unterstützen ihn unmittelbar in seinem beruflichen Wirkungskreis[18] und sind damit Teil einer einheitlichen Verantwortungssphäre, in der sich die Beteiligten gegenseitig vertrauen können müssen.[19] Hilfspersonen unterstehen denn auch der gleichen Strafdrohung wie der (Haupt-)Geheimnisträger. Eine Bekanntgabe der Geheimnisse an Hilfspersonen oder deren Kenntnisnahme erfüllt das objektive Tatbestandsmerkmal des Offenbarens an unberechtigte Dritte deshalb von vornherein nicht.[20]

C) Unberechtigte Dritte

Unberechtigte Dritte sind alle Personen, die weder Hilfspersonen sind noch von Gesetzes wegen oder aufgrund einer Einwilligung vom Geheimnis Kenntnis erlangen dürfen. Der Geheimnisträger kann das Berufsgeheimnis auch durch Weitergabe der geheimen Informationen an andere Schweigepflichtige verletzen, etwa durch Mitteilung an Anwältinnen oder Anwälte, die in einer anderen Anwaltskanzlei tätig sind.[21]

4. Konsequenzen für die Nutzung von Cloud-Computing

A) Cloud-Provider als Hilfspersonen

Aus den vorstehenden Ausführungen ergibt sich, dass Cloud-Provider als Hilfspersonen von Anwältinnen und Anwälten im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB zu qualifizieren sind. Ihnen dürfen die durch das Berufsgeheimnis geschützten Informationen zugänglich gemacht werden, ohne dass ein unzulässiges Offenbaren vorliegt.[22]

B) Sorgfaltspflichten bei Auswahl, Instruktion und Überwachung

Bei der Auswahl der Hilfsperson müssen die Berufsgeheimnisträger gewisse Regeln beachten, die sich auch aus dem Zivil- und Berufsrecht ergeben.[23] Das Berufsrecht kann zwar kein Offenbaren erlauben, das strafrechtlich verboten ist,[24] aber es kann dazu beitragen, den Begriff der Hilfsperson von Art. 321 Ziff. 1 Abs. 1 StGB im Rahmen einer teleologischen Auslegung zu konkretisieren.

Wenn Anwältinnen oder Anwälte Hilfspersonen beiziehen, haften sie nach Art. 101 OR für alle in Erfüllung der Schuldpflicht durch ihre Hilfspersonen verursachten Schäden, sofern ihnen diese hypothetisch vorwerfbar sind. Art. 13 Abs. 2 BGFA verlangt zudem, dass Anwältinnen und Anwälte durch Auswahl, Instruktion und Überwachung ihrer Hilfspersonen für die Wahrung des Berufsgeheimnisses sorgen.[25] Wenn sie nicht alles Zumutbare unternehmen, um die Wahrung des Geheimnisses sicherzustellen, verstossen sie gegen diese Berufsregel.[26] Die Lehre fordert denn auch, dass Hilfspersonen vertraglich zur Geheimhaltung verpflichtet werden,[27] und betont zugleich, dass je nach Grösse und Tätigkeit der Kanzlei ein eigentliches Sicherheitsdispositiv erforderlich ist.[28] Es kann sich deshalb aufdrängen, bei besonders sensiblen Informationen den Kreis der einbezogenen Hilfspersonen enger zu fassen und angemessene technische und organisatorische Massnahmen zum Schutz der Informationen zu ergreifen.

Der Geheimnisträger ist in seinem Vorgehen damit nicht völlig frei. Die Beachtung der zivil- und berufsrechtlichen Pflichten erfordert vielmehr eine sinnvolle Begrenzung des Personenkreises, der Zugang zu den geheimen Informationen erhält, und das Ergreifen ausreichender Massnahmen zu deren Absicherung.

---

18 DONATSCH/THOMMEN/WOHLERS (Fn. 14), 590; KELLER (Fn. 13), 107 f. m. w. H.

19 TRECHSEL/VEST (Fn. 2), StGB 321 N 25. Siehe dazu auch die zivilrechtliche Regelung betreffend Haftung für Handlungen der Hilfsperson, Art. 101 OR: WIEGAND, in: Basler Kommentar OR I, 6. Aufl., Basel 2015, OR 101 N 4 f. So auch BezGer Zürich, Urteil vom 18. 11. 2015, GG 150233, E. II.2.5.3.

20 Explizit: BezGer Zürich, Urteil vom 18. 11. 2015, GG 150233, E. II.2.5.3; sowie STRATENWERTH/WOHLERS, Schweizerisches Strafgesetzbuch Handkommentar, 3. Aufl., Bern 2013, StGB 320 N 3, StGB 321 N 4. A. M. WOHLERS (Fn. 5), 21 f., 25 f.: «Tatsächlich kann (…) aus der Existenz der Kategorie der Hilfspersonen als taugliche Täter *nicht* gefolgert werden, dass auch die Weitergabe an sie *für den primären Geheimnisträger* straflos sein soll. Die Kategorisierung als Hilfsperson ändert deshalb für sich gesehen nichts daran, dass die Weitergabe der Daten als Offenbaren eines Geheimnisses einzustufen ist» (Hervorhebung durch die Verfasser).

21 BGE 114 IV 44, E. 3.b; BERGER (Fn. 17), 187; DONATSCH/THOMMEN/WOHLERS (Fn. 14), 593 m. w. H.; ISENRING (Fn. 14), StGB 320 N 15, StGB 321 N 10; KELLER (Fn. 13), 114 f. m. w. H.; PIETH, Strafrecht, Besonderer Teil, 2. Aufl., Basel 2018, 131; RASELLI, Amts- und Rechtshilfe durch Informationsaustausch zwischen schweizerischen Straf- und Steuerbehörden, ZStrR 1993, 32 f. m. w. H.; STRATENWERTH/BOMMER (Fn. 2), § 61 N 7.

22 A. M. WOHLERS (Fn. 5), 20, der Outsourcingnehmer nicht als Hilfspersonen betrachtet. Sobald sie die geheimen Informationen des Geheimnisherrn entschlüsseln können, geht er von einem Offenbaren aus. Ebenso bezüglich IT-Dienstleistern, welche die Wartung von Software übernehmen.

23 WOHLERS (Fn. 5), 16, sowie WOHLERS (Fn. 13), 115, ist aufgrund seines engen Auslegungsansatzes der Ansicht, dass die Kontrolle über den Kreis der Geheimnisberechtigten nicht dem Anwalt bzw. der Anwältin überantwortet werden könne.

24 NATER/ZINDEL (Fn. 13), BGFA 13 N 16; siehe auch: WEBER, in: Basler Kommentar OR I, 6. Aufl., Basel 2015, OR 398 N 11.

25 SCHILLER, Schweizerisches Anwaltsrecht, Zürich 2009, Rn. 540 ff.; siehe auch: CHAPPUIS/ALBERINI (Fn. 13), 341.

26 SCHILLER (Fn. 25), Rn. 540; NATER/ZINDEL (Fn. 13), BGFA 13 N 56 f.

27 MAURER/GROSS, in: Commentaire romand, Loi sur les avocats, LLCA, Basel 2010, LLCA 13 N 101; SCHILLER (Fn. 25), Rn. 541; NATER/ZINDEL (Fn. 13), BGFA 13 N 56; siehe auch DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Tätigkeitsbericht 2017, 18.

28 NATER/ZINDEL (Fn. 13), BGFA 13 N 56 f. Zu denken wäre z. B. an das Schlüsselmanagement, das bei IaaS-Dienst-Modellen in der Verantwortung der Kanzlei bleibt (siehe II. 2) II. 1. A) oder die Zugangskontrolle bei IaaS- und SaaS-Dienst-Modellen, die immer in der Verantwortung der Kanzlei bleibt (siehe II. 1. B).

C) Beizug ausländischer Cloud-Provider

Werden Daten ins Ausland transferiert oder wird einem ausländischen Cloud-Provider der Zugriff auf in der Schweiz gespeicherte Daten ermöglicht, unterstehen diese Daten unter Umständen einem schwächeren rechtlichen Schutz oder einem Zugriffsrecht ausländischer Behörden (z. B. bei strafprozessualen Zwangsmassnahmen). So ermöglicht z. B. der im März 2018 vom US-Kongress erlassene Cloud Act[29] US-Behörden den Zugriff auf im Ausland gespeicherte Daten, wenn sich diese im Besitz, Gewahrsam oder unter der Kontrolle eines US-amerikanischen Cloud-Providers befinden.[30]

Die Schweizer Strafhoheit knüpft grundsätzlich am Begehungsort an, d. h., entweder am Ausführungs- oder am Erfolgsort (Art. 8 Abs. 1 StGB). Wird das Geheimnis im Ausland offenbart und dort zur Kenntnis genommen, kann es an einem Schweizer Begehungsort fehlen. Für die Zulässigkeit einer Bekanntgabe an eine Hilfsperson ist aber nicht entscheidend, dass diese auch selbst Art. 321 StGB untersteht.[31] Entscheidend ist vielmehr, dass der Beizug des Cloud-Providers berechtigt ist. Dies bedingt, dass dieser vertraglich zur Wahrung des Berufsgeheimnisses verpflichtet ist und die Auslagerung einer Risikobeurteilung im Einzelfall standhält.[32] Bei dieser Beurteilung ist vor allem die Sensitivität der Daten, aber auch die zu erwartende Vertrags- und Gesetzestreue des ausländischen Cloud-Providers sowie die tatsächliche Wahrscheinlichkeit eines Zugriffs auf die Daten zu berücksichtigen. Diese Risikoeinschätzung kann je nach Tätigkeit von Anwältinnen und Anwälten unterschiedlich ausfallen; besondere Vorsicht dürfte etwa bei der Beratung ausländischer Klienten in Steuerfragen und bei politisch exponierten Mandanten angezeigt sein.

5. Zusätzliche Absicherung: rechtfertigende Einwilligung

Auch wenn die Nutzung von Cloud-Providern durch Anwältinnen und Anwälte grundsätzlich zulässig ist, erscheint es im Sinn einer zusätzlichen Absicherung sinnvoll, von den Klienten im Rahmen des Mandatsvertrages eine Einwilligung zur Nutzung von Cloud-Providern (wie auch zum Einsatz weiterer Hilfspersonen, etwa Substituten und IT-Verantwortlichen) einzuholen. Diese Einwilligung kann formlos erteilt werden. Von einer konkludenten Einwilligung liesse sich zudem ausgehen, wenn die Klienten über die Nutzung von Cloud-Diensten hinreichend informiert wurden und sie das Mandatsverhältnis ohne Weiteres fortführen. Für abgeschlossene Mandatsverhältnisse bietet sich dagegen eine nutzerseitig verschlüsselte Archivierung im Rahmen eines IaaS-Dienst-Modells an, die einen Zugriff des Cloud-Providers auf die Daten im Klartext von vornherein ausschliesst (siehe II. 2).

IV. Datenschutzrechtliche Beurteilung: Auftragsdatenbearbeitung

1. Bearbeiten von Personendaten

Das Bearbeiten personenbezogener Daten, also von Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, untersteht den Vorgaben des Datenschutzrechts (Art. 2 i. V. m. Art. 3 lit. a DSG).

Keine Anwendung findet das Datenschutzrecht auf die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, wenn die Cloud-Provider keine Personendaten bearbeiten. Dies ist der Fall, wenn die Daten beim Cloud-Provider lediglich gespeichert werden (IaaS-Dienst-Modell) und die Anwältinnen und Anwälte die Daten vor der Übermittlung an den Provider verschlüsseln, sodass dieser keinen Zugriff auf die Daten im Klartext hat. Anderes gilt, wenn Anwältinnen und Anwälte die Daten auf der Infrastruktur von Cloud-Providern (SaaS-Dienst-Modell) bearbeiten, weil die Cloud-Provider hier auf die Daten zugreifen können (siehe II. 2).

Gemäss Lehre und Rechtsprechung liegen personenbezogene Daten vor, wenn nach der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass der Bearbeiter den Aufwand auf sich nehmen wird, um eine Person zu bestimmen.[33] Da dies bei der Nutzung von Cloud-Providern nach dem SaaS-Dienst-Modell nicht ausgeschlossen werden kann, ist die Nutzung dieser Dienste durch Anwältinnen und Anwälte als Bearbeiten von Personendaten zu qualifizieren, das nach den Vorgaben des DSG zu erfolgen hat.

2. Auftragsdatenbearbeitung

A) Verantwortung beim Auftraggeber

Soweit die Bearbeitung von Personendaten durch die Anwältinnen und Anwälte zulässig ist und die Voraussetzungen der Auftragsdatenbearbeitung nach Art. 10a DSG erfüllt sind, dürfen die Daten auch durch den Cloud-Provider bearbeitet werden. Die Anwältinnen und Anwälte bleiben jedoch als Auftraggeber für die Einhaltung der Vorgaben des Datenschutzrechts verantwortlich.[34]

B) Übertragung durch Vereinbarung

Bei der Auftragsdatenbearbeitung beruht die Bearbeitung personenbezogener Daten auf einer Vereinbarung (Cloud-Vertrag) zwischen den Anwältinnen und Anwälten bzw.

---

29 Clarifying Lawful Overseas Use of Data Act. Der Cloud Act ist eine Reaktion auf das Urteil in Sachen Microsoft v. United States, *829 F.3d 197 (2d Cir. 2016),* mit dem der Court of Appeal for the Second Circuit entschieden hat, dass das FBI Microsoft nicht zur Herausgabe von Daten verpflichten könne, wenn diese auf einem Server in Irland gespeichert sind. Siehe auch 130 Harv. L. Rev. (2016), 769 ff.

30 GAUSLING, Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, 579.

31 A. M. SCHWANINGER/LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, Jusletter 11. März 2013, Rn. 31 f.

32 Siehe vorn, III. 4. B).

33 Siehe dazu: BGE 136 II 508, E. 3.

34 GRAMIGNA, Cloud-Vertrag, in: Schweizerisches Vertragshandbuch: Musterverträge für die Praxis, 3. Aufl., Basel 2017, Rn. 30; BAERISWYL, in: Stämpflis Handkommentar Datenschutzgesetz, Bern 2015, DSG 10a N 2; BÜHLER/RAMPINI, in: Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, DSG 10a N 11; SURY/GOGNIAT, Umzug einer Kanzlei in die Cloud, AwR 2015, 204.

deren Kanzlei und dem Dienstleister, hier also dem Cloud-Provider.

C) Bearbeitung wie Auftraggeber

Die Anbieter von Cloud-Diensten dürfen die von den Anwältinnen und Anwälten übermittelten Personendaten nur so bearbeiten, wie es diese als Auftraggeber auch selbst tun dürften (Art. 10a lit. a DSG). Soweit die Vorgaben des Datenschutzrechts eingehalten sind, die Bearbeitung der Personendaten durch die Anwältinnen und Anwälte also namentlich die Grundsätze der Datenbearbeitung einhält oder auf einem Rechtfertigungsgrund beruht, dürfen die Daten nicht nur von den Anwältinnen und Anwälten, sondern auch von den Cloud-Providern bearbeitet werden. Unzulässig wäre hingegen eine Bearbeitung durch die Cloud-Provider zu eigenen Zwecken.[35] Um sicherzustellen, dass der Cloud-Provider die Daten nicht anders bearbeitet als die Anwältinnen und Anwälte, sollte die Art der Bearbeitung der Daten durch den Cloud-Provider im Cloud-Vertrag oder in einem Annex dazu geregelt werden.[36] Dabei kann z. B. festgehalten werden, dass die Daten – unter Vorbehalt besonderer Weisungen – nur zur Vertragserfüllung bearbeitet werden dürfen.[37]

D) Keine entgegenstehenden Geheimhaltungspflichten

Die Bearbeitung von Personendaten durch Dritte ist unzulässig, wenn gesetzliche oder vertragliche Geheimhaltungspflichten bestehen und nicht eingehalten werden (Art. 10a Abs. 1 lit. b DSG).[38] Wie vorstehend aufgezeigt,[39] liegt bei der Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte kein Verstoss gegen gesetzliche Geheimhaltungspflichten vor. Denkbar ist allerdings, dass vertraglich eine Pflicht zur Geheimhaltung vorgesehen wird, die einer Auslagerung entgegensteht.

E) Gewährleistungs- und Überwachungspflichten, insbesondere Datensicherheit

Da die Anwältinnen und Anwälte für die Einhaltung der Vorgaben des Datenschutzrechts verantwortlich bleiben,[40] sind sie zur sorgfältigen Auswahl, Instruktion und Überwachung des Cloud-Providers verpflichtet.[41] Sie müssen insbesondere sicherstellen, dass der Cloud-Provider die Datensicherheit (Art. 10a Abs. 2 DSG), d. h. die Vertraulichkeit, Verfügbarkeit und Integrität der Daten, gewährleistet (Art. 8 Abs. 1 VDSG). Für diese Beurteilung kann ein unabhängiger Spezialist beigezogen werden, der das Sicherheitsdispositiv des Cloud-Providers prüft.[42] Es kann aber auch auf ein zertifiziertes Qualitätsmanagementsystem des Cloud-Providers nach ISO 9001 bzw. ISO 27001 oder auf eine datenschutzspezifische Zertifizierung (z. B. GoodPriv@cy, VDSZ:2014 oder ePrivacy) vertraut werden.

3. Auslagerung ins Ausland

Können Personen ausserhalb der Schweiz auf die in der Cloud gespeicherten Daten zugreifen (insb. bei der Nutzung eines ausländischen Cloud-Providers, aber auch im Rahmen einer Fernwartung), liegt eine grenzüberschreitende Bekanntgabe von Daten vor (Art. 6 DSG)[43]. Existiert im fraglichen Land eine angemessene Datenschutzgesetzgebung, ist dies datenschutzrechtlich grundsätzlich unproblematisch (Art. 6 Abs. 1 DSG). Der EDÖB veröffentlicht gemäss Art. 7 VDSG eine Liste der Staaten, die vermutungsweise einen angemessenen Datenschutz gewährleisten.[44] Für Staaten, die nicht auf dieser Liste stehen, wie etwa die USA, müssen sich Anwältinnen und Anwälte hinreichende Garantien hinsichtlich des Datenschutzes geben lassen. Solche Garantien können vertraglicher Natur sein oder in der Selbstzertifizierung des Cloud-Providers unter dem Swiss-US Privacy Shield bestehen.[45]

4. Exkurs: Datenschutzgrundverordnung (DSGVO)

Auf die Tätigkeit von Schweizer Anwältinnen und Anwälten kann die Datenschutzgrundverordnung (DSGVO) der EU Anwendung finden, namentlich wenn die Anwältinnen und Anwälte ihre Tätigkeit (auch) auf Klienten aus der EU ausrichten (Art. 3 Abs. 2 DSGVO)[46]. Die Anwendbarkeit der DSGVO kann sich aber auch aus dem IPRG ergeben, weil der Verletzte bei Persönlichkeitsverletzungen das Recht am Aufenthalts- oder Erfolgsort wählen kann, wenn mit einem Schadenseintritt in diesem Land zu rechnen war (Art. 139 Abs. 3 i. V. m. Abs. 1 IPRG). Auf eine persönlichkeitsverletzende Bearbeitung von Personendaten in einer

---

35 BAERISWYL (Fn. 34), DSG 10a N 26.
36 ROSENTHAL, in: Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008, DSG 10a N 71.
37 ROSENTHAL (Fn. 36), DSG 10a N 72.
38 BAERISWYL (Fn. 34), DSG 10a N 29; gl. M.: WOHLERS (Fn. 13), 115.
39 Siehe vorn, III. 4.
40 Siehe vorn, IV. 2. A).
41 Siehe BBl 1988 II 413, 463 f.
42 SURY/GOGNIAT (Fn. 34), 203.
43 BGE 144 I 126, E. 8.3.6; ROSENTHAL (Fn. 36), DSG 6 N 7; BÜHLER/RAMPINI (Fn. 34), DSG 10a N 22d; GRAMIGNA, Datenschutz und Outsourcing, in: Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, Rz. 20.24; STRAUB, Cloud Verträge – Regelungsbedarf und Vorgehensweise, AJP 2014, 914; SCHWANINGER/LATTMANN (Fn. 31), Rn 15.
44 Siehe https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf., zuletzt besucht am 7. November 2018; OGer ZH, Urteil vom 3. März 2015, LF140075, E. 3.2; PASSADELIS, Rechtsanwendung bei internationalen Datenbearbeitungen durch Private, in: Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, Rz. 6.44.
45 Siehe: EDÖB, Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html, sowie die Liste des Swiss-US Privacy Shield zertifizierten Unternehmen des US Department of Commerce, https://www.privacyshield.gov/list, beide zuletzt besucht am 7. November 2018.
46 Im Einzelnen ZERDICK, in: Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, 2. Aufl., München 2018, DSGVO 3 N 19; siehe DSGVO, Erwgr. 23 sowie EuGH, Urteil vom 7. 12. 2010, C-585/08 und C-144/09, Pammer/Alpenhof zur Auslegung des Begriffs des Ausrichtens einer Tätigkeit. Siehe ferner PRAZ, Responsabilités et outils de conformité selon la RGPD: Obligations du responsable de traitement et du sous-traitant, AJP 2018, 610; VASELLA, Zum Anwendungsbereich der DSGVO, digma 2017, 220 ff.

Cloud könnte die DSGVO namentlich als Recht des Aufenthaltsorts des Klienten Anwendung finden, zumal ein Erfolgseintritt am gewöhnlichen Aufenthaltsort des Klienten in der Regel vorhersehbar ist.[47]

Die Rechtslage für die Auslagerung einer Datenverarbeitung nach Art. 28 DSGVO entspricht in den Grundzügen derjenigen nach dem DSG. Die Auslagerung im Rahmen der Auftragsdatenverarbeitung wird privilegiert und muss nicht durch einen eigenständigen Erlaubnistatbestand nach Art. 6 DSGVO abgedeckt sein.[48] Art. 28 DSGVO gibt aber im Unterschied zum DSG sehr detailliert vor, wie der Auftraggeber seine Pflichten bei der Auftragsdatenverarbeitung einzuhalten hat.[49] Der Auftragsdatenverarbeiter ist zudem ein Empfänger im Sinn von Art. 4 Nr. 9 DSGVO, wenn ihm Daten offengelegt werden. Der Verantwortliche muss die betroffenen Personen über die Empfänger von Daten informieren (Art. 13 Abs. 1 lit. e DSGVO; Art. 14 Abs. 1 lit. e DSGVO), wobei ein Bereitstellen der Information, z. B. in einer über das Internet abrufbaren Datenschutzerklärung, genügt.[50]

V. Fazit

Werden Daten durch Anwältinnen und Anwälte vor der Übertragung an einen Cloud-Provider verschlüsselt und verfügt der Cloud-Provider nicht über den Schlüssel, liegt kein Offenbaren von Geheimnissen im Sinn von Art. 321 StGB vor. Da verschlüsselte Daten nicht als Personendaten zu qualifizieren sind, untersteht die Tätigkeit des Cloud-Providers auch nicht dem Datenschutzrecht. In dieser Konstellation ist die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte deshalb straf- und datenschutzrechtlich unbedenklich.

Werden die Daten aber nicht durch die Anwältinnen und Anwälte, sondern erst durch den Cloud-Provider verschlüsselt, hat dieser Zugriff auf die Daten im Klartext und Zugang zu den vom Berufsgeheimnis geschützten Informationen. Mit der Nutzung seiner Dienste wird der Cloud-Provider allerdings Teil der arbeitsteilig organisierten Funktionseinheit «Anwaltskanzlei» und ist damit als Hilfsperson der Anwältinnen und Anwälte zu qualifizieren. Hilfspersonen sind nie unberechtigte Dritte im Sinn von Art. 321 StGB. Die Bekanntgabe geheimer Informationen an Cloud-Provider erfüllt deshalb das objektive Tatbestandsmerkmal des Offenbarens an unberechtigte Dritte nicht, womit eine Strafbarkeit nach Art. 321 StGB entfällt. Anwältinnen und Anwälte müssen den Cloud-Provider allerdings sorgfältig auswählen, die Wahrung des Berufsgeheimnisses vertraglich absichern und sicherstellen, dass die Daten vom Cloud-Provider nur zur Vertragserfüllung verwendet werden. Die Einhaltung dieser Verpflichtungen ist in zumutbarer Weise zu überwachen. Auch aus Sicht des Datenschutzrechts ist die Nutzung von Cloud-Providern als Auftragsdatenbearbeiter der Anwältinnen und Anwälte grundsätzlich unproblematisch, weil das Berufsgeheimnis der Auftragsdatenbearbeitung nicht entgegensteht. Werden auch die weiteren Vorgaben der Auftragsdatenbearbeitung eingehalten, kann der Cloud-Provider die Daten so bearbeiten, wie die Anwältinnen und Anwälte es auch selbst tun dürfen.

---

47 ROSENTHAL (Fn. 36), IPRG 139 N 26; BÜHLMANN/REINLE, Extraterritoriale Wirkung der DSGVO, digma 2017, 10. Zur Anwendung kämen die DSGVO sowie das nationale, die DSGVO umsetzende Recht.

48 PLATH, in: DSGVO/BDSG-Kommentar, 3. Aufl., Köln 2018, DSGVO 28 N 6; SCHMIDT/FREUND, Perspektiven der Auftragsdatenverarbeitung – Wegfall der Privilegierung mit der DS-GVO?, ZD 2017, 16.

49 Art. 28 DSGVO könnte daher auch eine Orientierungshilfe für Schweizer Datenbearbeiter bieten.

50 LAUE/NINK/KREMER, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016, § 3 N 17; siehe auch: KAMLAH, in: DSGVO/BDSG-Kommentar, 3. Aufl., Köln 2018, DSGVO 12 N 4.